Appl. No.   :   09/755,452
Filed   :   January 5, 2001

REMARKS

Reconsideration and allowance of the above-referenced application are respectfully requested.

Claims 1, 9,14, 15, 16 and 21 stand rejected under 35 U.S.C. 102 as allegedly being anticipated by Orita. This contention, however, is respectfully traversed.

Orita does teach a system of file security, but uses a completely different kind of security than that defined by the present claims.

Claim 1 requires identifying the user and designating a first plurality of files in a computer as associated with the user. If the user is identified, then the user can make a change to the first plurality of files, those that are associated with the user. When the user is not identified, the first plurality of files cannot be read by the user.

Orita's computer system does have a file security function. The user enters their ID information (see for example column 3 line 10) to allow access to the computer itself. However, according to Orita, the security is the security of a file, not the security of the user. Moreover, the files are each associated with security such as passwords, but the files are not associated with a user, as claimed.

Columns 1-2 as identified by the rejection described how operator profile information corresponds to ID information, e.g. user information. This is the information that the user needs, in order to log in. However, nowhere is there any teaching or suggestion that a user can make changes to the first plurality of files that are associated with the user, but cannot read contents of the files when the user (with whom the files are associated) is not identified. According to Orita, each file gets a special kind of security; see generally column 3 line 57 through column 4 line 22. The file may have a

-8-

Appl. No.   :   **09/755,452**
Filed   :   **January 5, 2001**

file password, see column 4 line 21. The user enters their information name and their

ID information and is allowed access to the file based on whether the EP information is

correct or not. This EP information, however, is the EP password, the EP authority

level, program name, filename, and file password. See generally column 3 lines 56-60.

While the user must have access to the system in order to get to the files, the access

information is based on a password and file type of each file. See generally column 4

lines 55-60. Therefore, the files are not associated with specific users as defined by

claim 1, but rather are associated with passwords and other kinds of "EP" information.

As such, Orita does not describe "designating the first plurality of files in a computer as

being associated with said user" as claimed. Orita therefore, does not describe claim 1

and therefore claim 1 should be allowable.

Claim 14 requires has been amended to include the limitations of claim 17

therein, thereby obviating the rejection over Orita.

Claims 2-7, 10, 12, 13, 17, 18-20 and 22-27 stand rejected under 35 USC 103 as

allegedly being unpatentable over Orita in view of Tello. This contention is further

respectfully traversed.

Claim 2 defines that the "preventing the contents from being read" comprises

encrypting the files. While encryption per se is known, it is respectfully suggested that

there is no teaching or suggestion of using encryption to prevent access to files that are

not associated with the user, as claimed.

Tello does teach that part of the device driver layer on the motherboard allows

data to be encrypted or decrypted before being passed to the peripheral. Nowhere is

there any teaching or suggestion that the files are encrypted, to "prevent reading

-9-

Appl. No.   :   09/755,452
Filed   :   January 5, 2001

contents" and that a user who is associated with the files can read those files. Simply teaching that files can be encrypted before being passed to a peripheral does not teach or suggest this subject matter. This is different than passing encrypted information to a motherboard – this defines, instead, encrypting files so that only the user who is associated with those files, can read them.

Claim 4 requires that the unique information, (which is amended herein for proper antecedent) includes a unique number indicative of hardware in the computer system. Tello does teach a unique number, but it is used for identification of the computers, not for encryption

Claim 4 is further allowable since it defines unencrypted information in read-only files, but no changes to be made as well as encrypted information and read/write files. Orita teaches absolutely nothing about this subject matter. Nowhere is there any teaching or suggestion of read/write files being encrypted, but read only files being unencrypted. These claims should therefore be additionally allowable.

Claim 10 should be allowable for similar and analogous reasons. Specifically, claim 10 requires that the unencrypted files are read only, and that the encrypted files are read/write files. In this way, file security is maintained. A user, or more importantly an unauthorized user such as a virus or hacker, can not change the files unless the user has the encryption key. That user, or any other user, however, can read the read-only files, but cannot change them. This is nowhere taught or suggested by the cited prior art. The prior art simply teaches both encrypted and unencrypted files within the same system, but teaches nothing about this specific subject matter.

-10-

Appl. No.   :   09/755,452
Filed   :   January 5, 2001

Claim 17, now incorporated into claim 14, defines that the access is controlled by encryption in the files. Nowhere is there any teaching or suggestion of this in Orita in view of Tello. The hypothetical combination would teach an Orita type system that had file security functions, along with a Tello type motherboard which used encryption before sending to peripherals. Claim 22 should hence be allowable for reasons discussed above. Nowhere is there any teaching or suggestion of allowing the user to make changes to files using an encryption system, based on the files being associated with the user, but allowing unencrypted files to be read, while preventing writing to those files. Claim 22 also requires special files that are unencrypted but can be written to or read from.

Claim 23 defines encrypting all files other than specified files, and should be allowable for reasons discussed above.

The dependent claims should be allowable for similar reasons to those discussed above with respect to the respective independent claims. Claim 8 specifically rejected based on Orita in view of Portero. Admittedly Portero teaches logging access attempts, but teaches nothing about the subject matter discussed above.

Finally, with all due respect, one having ordinary skill in the art would not make the hypothetical combination of Orita in view of Tello in the way suggested by the Official Action. The Official Action apparently suggests that the file security function of Orita should be modified by the motherboard structure of Tello. However, Tello refers a way that the motherboard produces output signals for use with other hardware. It teaches nothing about file security. The hypothetical combination of Tello and Orita is

-11-

Appl. No.   :   09/755,452
Filed   :   January 5, 2001

made entirely based on hindsight. In fact, one reading the two references together would obtain guidance only to use a computer system encryption before sending to peripheral devices. Nowhere would there be any suggestion of encrypting files to restrain access, or the other features which have been described in detail above.

It is believed that all of the pending claims have been addressed in this paper. However, failure to address a specific rejection, issue or comment, does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above are not intended to be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Appl. No.   :   09/755,452
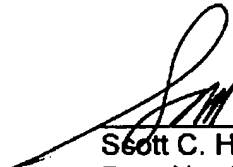Filed   :   January 5, 2001

Therefore, and in view of the above amendments and remarks, all of the claim

should be in condition for allowance. A formal notice to that effect is respectfully

solicited.

Please charge any fees due in connection with this response to Deposit Account

No. 50-1387.

Respectfully submitted,

Date: 5/27/05

Scott C. Harris
Reg. No. 32,030

Customer No. 23844
Scott C. Harris, Esq.
P.O. Box 927649
San Diego, CA 92192
Telephone: (619) 823-7778
Facsimile: (858) 678-5082

-13-